Volume 17, Issue 12   Atari Online News, Etc.   March 20, 2015

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1712   03/20/15

~ Net Neutrality Control ~ People Are Talking!   ~ Atari Devs on 2600!
~ Silk Road’s Nash Plea! ~ Spartan, IE Alternative ~ Browsers Exploited!
~ Double FREAK! New Bug! ~ OpenSSL Leak Patched!   ~ WHOIS Data Leaked!

~ New Facebook Guidelines ~ Windows 10 in Summer?   ~ Pirates Beware Win10!

-* Atari Says No to Minter’s TxK *-
-* Internet of Things (IoT) Cyberattack *-
-* China Finally Admits It Has Army of Hackers *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Welcome Spring! Bah! Look outside, it’s snowing again here in New England! So much for that long-awaited feel-good date on the calendar! We knew it was too good to be true; and the cold and snow keeps managing to prove it to us. Not much we can do about it, so let’s all sit back and relax in a nice warm, cozy seat and enjoy another week’s issue!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Atari Says No to Minter’s TxK!
"""""""""""""""""""""""""""""   Atari Devs Dissect Yars Revenge!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Atari Spikes Plans To Launch Tempest Successor on PS4, Creator Says

Jeff Minter’s TxK, a spiritual successor to the Tempest franchise he worked on for Atari in the 1990s, will not release on PlayStation 4, Windows PC and Android following a copyright claim and shutdown demand from Atari, Minter said.

Minter said via Twitter this morning that he is "beyond disgusted" by Atari’s actions, which end plans to release the game on three additional platforms a year after it launched on the PS Vita. In promoting the game, Minter had said that TxK would "do for (Tempest 2000) what T2K itself did for its ancient arcade ancestor." Minter was producer on

Tempest 2000, which was released in 1994 for Atari’s Jaguar console.

TxK still is listed on the PlayStation Store at $9.99. On his personal blog, Minter wrote that Atari is "still trying to insist that I remove from sale Vita TxK."

Polygon has reached out to an Atari representative for comment and will update this story with any reply.

Update: Atari says it was "surprised and dismayed by the very close similarities between TxK and the Tempest franchise," when it launched last year, noting that "several major gaming outlets," expressed the same opinion. ("This is essentially Tempest," IGN said in its review at the time.)

Update 4:55 p.m. In comments to Kotaku, Minter disputes that Atari ever contacted him about TxK, saying he does not consider communication from Atari’s attorneys to be contact from Atari itself. (This letter, dated June 2014, shows Atari contacted him about NxT on April 1, 2014; moreover, Minter’s attorney replied.) He says he tried to initiate backchannel contact with Atari over NxT ("We did try to approach them via a non-lawyer route," he says) but was unsuccessful.

Minter founded Llamasoft, the studio developing TxK. It also developed Space Giraffe, a 2007 Xbox Live Arcade release that echoed Tempest’s gameplay.

On his blog, Minter says that the two sides had been in discussions "for a while now," and that he had hopes "we could maybe work something out, maybe Atari’ would commission an officially licensed version from us; we made it clear we’d be willing to negotiate about that sort of thing."

Instead, Minter says, Atari lawyers accused him of   among other things having access to and stealing source code from Tempest 2000 to create TxK, and also alleged that TxK’s soundtrack was a ripoff of Tempest 2000 (it is original, Minter said.)

Minter said he consulted a lawyer and they said it would be very expensive to contest all of the claims Atari was making. He said Atari demanded that he "sign papers basically saying I can never make a Tempest style game ever again."

Atari notes that "there is no lawsuit," although Minter said only he felt threatened by legal proceedings. "Atari has been in continuous contact with the developer since the game launched in hopes that the matter would be resolved," Atari said.

So yeah all the stuff we had ready or near ready will now never see the light of day.No TxK PC, PS4, Oculus, GearVR, Android. Thank "Atari".

Jeff Minter (@llamasoft_ox) March 18, 2015

The quote marks around Atari reference the fact the brand has been sold and reorganized repeatedly over the past two decades, including a 2013 bankruptcy. A year ago it announced a push into mobile and social gaming with Atari Casino, which draws on longtime trademarks it owns like Missile Command and Centipede. It later announced a partnership with a lottery game developer to bring those brands to real-money gambling formats.

But I could never have imagined one day being savaged by its undead corpse, my own seminal work turned against me. I am beyond disgusted.
Jeff Minter (@llamasoft_ox) March 18, 2015

Atari Blocking TxK On All Platforms, Says Creator Jeff Minter

"Atari values and protects its intellectual property and expects others to respect its copyrights and trademarks. When Llamasoft launched TxK in early 2014, Atari was surprised and dismayed by the very close similarities between TxK and the Tempest franchise. Atari was not alone in noticing the incredible likeness between the titles. Several major gaming outlets also remarked at the similarity of features and overall appearance of TxK to Tempest; one stated of TxK, 'This is essentially Tempest.' There is no lawsuit. Atari has been in continuous contact with the developer since the game launched in hopes that the matter would be resolved."

The quote from Atari's statement comparing TxK to Tempest is from IGN's own review of TxK from last year.

TxK, the colorful PS Vita tube shooter from Llamasoft, won't be coming to additional platforms according to creator Jeff Minter, who says Atari is blocking the game on legal grounds.

A series of tweets from Minter, beginning yesterday, marks this as an ongoing, year-long battle that is just now going public.

One of Minter's earliest tweets about the situation refers to "forces hostile to Llamasoft" that have been "bullying" his company over the similarity between his game TxK and Atari's Tempest games.

"So yeah all the stuff we had ready or near ready will now never see the light of day. No TxK PC, PS4, Oculus, GearVR, Android. Thank 'Atari'," tweeted Minter.

Minter used to work at Atari, where in 1994 he created Tempest 2000, an Atari Jaguar remake of Dave Theurer's classic Atari arcade game Tempest from 1984. TxK, which Minter released in 2014 on the PS Vita, is not an official remake or sequel of Tempest 2000.

In a PlayStation blog post from 2013, Minter referred to it as a "new game in a similar vein" that "will draw on the spirit of the classic T2K."

It seems this is enough for Atari to make accusations against Minter, who says that Atari is accusing him of stealing "Atari secrets" and plagiarizing the Tempest 2000 soundtrack.

Minter continues to express his disappointment over the ordeal, stating: "IDK why it's fine for others to clone T2K but as the original creator I get handed the shaft for a distantly related sequel."

In a blog post, re-posted on Pastebin due to the large amounts of traffic, Minter elaborates on some of the pressure he says Atari is putting on him, including removing TxK from the PlayStation store and signing away his rights to ever make a "Tempest style game" again.

Atari Lawyers Demand Vita Game TxK Is Removed

The PS Vita shooter TxK will not be released on PlayStation 4, PC, Oculus Rift, GearVR, or Android, due to its creator allegedly receiving legal pressure from Atari.

Jeff Minter, who previously worked at Atari when developing Tempest 2000, says the publisher is preventing him from releasing TxK onto other platforms due to copyright claims.

Atari released the first Tempest game in 1981, as part of a partnership with its original creator Dave Theurer. Then in 1994, it released Tempest 2000, which was developed by Minter. Twenty years later, Minter released TxK onto the PS Vita, a game which has demonstrably been inspired by the Tempest formula.

Due to its status as rights holder, Atari has issued Minter with legal documents alleging copyright theft. According to Minter s account of the situation, Atari has listed numerous similarities between Tempest 2000 and TxK.

According to Minter, Atari is also accusing him of deliberately setting out to cash in on Atari’s copyrighted Tempest name, by giving my game a deliberately obscure name of TxK."

Minter did not explain whether Atari is seeking damages, and was not able to respond to requests for comment at time of going to press. He did state, however, that the publisher wants the PS Vita version removed from sale.

 I think they thought I was somehow making loads and loads of money on the Vita version of TxK, I guess because it did garner excellent reviews and a bit of positive press. But the Vita isn’t a massive market, TxK made back its development advance and a bit more and that was it, he said.

 They kept hassling us and eventually I sent them sales statements so that they could see for themselves that we weren’t getting super rich out of it. I even tried to point out that if there was any serious money to be made out of it, it would likely be from the ports we were making, and that we were willing to negotiate about obtaining ’official’ branding for, if it meant they could at least be released, but we were met with nothing more than intransigence."

He continued: Even after having shown them that, they are still trying to insist that I remove from sale Vita TxK, even though it’s plainly at the end of its run now and only brings in a trickle these days, and sign papers basically saying I can never make a Tempest style game ever again. So no chance of releasing the ports."

Minter went onto describe Atari’s legal charges as all abject bollocks." and claims that the financial burden of answering these accusations in court would be too costly.

 Even just going back and forth a few times with letters responding to their threats ended up running up a couple of grand in legal bills, and there is simply no way on God’s earth I can afford any kind of a legal battle," he said.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
""""""""""""""""""""

Atari Devs Dissect Yars Revenge, Adventure, Atari s Woes

Like other Game Developers Conferences in the past, this year’s made sure to include a few meaty "post-mortem" panels hosted by legendary game designers. And with Atari er, what remains of it celebrating a huge 40th anniversary this year in the form of Pong’s first home edition, the company’s home console developers took center stage in the post-mortem pool.

"I’m going to tell you about the design of Adventure for the 2600, a game I designed in 1979," Warren Robinett said simply and plainly to introduce his own session. "Thank you. It was the first action-adventure game."

That’s no understatement. Adventure may seem painfully simple by today’s standards, but it wasn’t just the first "search a dungeon for treasure and fight monsters" game for home consoles; it actually friggin’ worked.

What Robinett pulled off with Adventure, especially on the piddling 2600 hardware, was unlike anything the gaming industry had ever seen before, and he isn’t blind to how much his game has been "widely imitated" ever since (even calling out The Legend of Zelda by name). More crucially, Robinett can easily confirm that he was the game’s sole creator, since, at the time, each 2600 game was produced entirely by one person.

"How many people have had a job where they re told, ’your job is to make video games, go make one’?" Robinett asked his GDC panel’s crowd. "That s what I heard on my first day of work, along with the fact that everyone in marketing was idiots."

In the fall of 1977, the 26-year-old Robinett was hired at Atari, where he debuted by producing the 2600’s Slot Racers a rudimentary racing game with a gun mechanic. For his next game, he wanted to create something much more inspired, so he turned to the most compelling game he’d played at the time: Colossal Cave Adventure, the "original text adventure game" made by Don Woods and Will Crowther exclusively for mainframe computers (which he’d luckily had access to).

With aspirations of making a similar game, full of traversal, items, and monsters, Robinett went to his Atari bosses and pitched a game inspired by CCA. Knowing that the mainframe text adventure required hundreds of kilobytes of memory, and that the 2600 only had 4K, he was told not to bother. "How many of you have been told not to work on something?" Robinett asked the GDC crowd. "How many of your bosses were wrong?"

Knowing he had roughly one month to secretly prototype his dream game, he focused on feasibility in his first build as in, proving he could get the

2600 to manage an quest-like game with six rooms, two objects, and one dragon. The fun would have to come later, but some of Adventure’s core concepts came about because of that feasibility effort. For example, Robinett tossed the idea of an "inventory screen" early on just as a memory concern, only to realize it also solved the 2600’s controller issue of having only one button. "I like the idea of staying in real time," Robinett said, as opposed to having a pause screen, "and limiting players to one object gave them a strategic choice weapon or treasure."

>From the sound of it, the development process’s biggest "a-ha" came when Robinett figured out a form of artificial intelligence for the game’s bats and dragons. It was a simple one, at that: they were each attracted to or repelled by certain objects, and a hierarchy governed which thing each object would react to first.

In all, the game contained 30 rooms, 14 objects and four creatures (three of which were color swaps for the dragon). He was then able to devote up to 40 bytes per room and up to 30 bytes per object. However, Robinett insists that he "never had to crunch Adventure" to make it fit in a cartridge. He pointed to his computer science education at Rice (undergrad) and UC Berkeley (graduate), and specifically at classes with Unix and C inventor Ken Thompson at the latter. "He required us to use C," he said. "It taught me to think like a C programmer."

As far as particularly technical stuff, Robinett talked at length about design decisions such as conserving RAM on the 2600, and he did so by "using a lot of variable-length data structures, because that didn’t waste any bytes," along with leaving a lot of inactive objects within the game’s ROM. "That let me only use RAM when I truly needed it," he said. Anybody truly curious about the game’s technical foundation may want to look up The Annotated Adventure, an e-book that he’s currently finishing. It will include the complete Adventure engine and for that effort, he translated the original Assembly code "by hand to C to make it more palatable." (During a Q&A portion, a few developers pleaded with Robinett to release the original Assembly code.)

Had Atari’s marketing team had its way, Adventure may have been cut off at the pass and turned into a Superman game shortly after the first prototype was completed. Atari’s John Dunn was actually tasked with taking that prototype code and slapping Superman into it, which meant Robinett could continue making his quest as he saw fit. Robinett also took a quick potshot at his former bosses:

"The big-money guys from New York didn’t succeed in controlling us 2600 programmers very well," he said. "They treated us so bad that we quit and started working at competing companies."

He didn’t otherwise speak at length about disagreements he had with Atari management, except to point out that he knew his name wasn’t going to be on the box and that he wouldn’t receive royalties. Thus, he made sure to sneak a "signature" into the code itself.

"I had to write my name within the limitations of the 2600," Robinett said as a screenshot of the game’s famed "easter egg" popped up on the screen, which read, "created by Warren Robinett." "Perhaps I wouldn’t be here today if I hadn’t done this sneaky trick." (Robinett also confirmed that he has since e-mailed with the first person to tip Atari off to the game’s secret room.)

Yars’ Revenge creator Howard Scott Warshaw benefited to some extent from that developer blowback, as he was the first Atari programmer to have his name printed on his game’s cartridge; what a difference three years makes. After being tasked with adapting Atari’s coin-op game Star Castle as a home game, Warshaw pushed back "though I’m a firm believer that you don’t complain without solutions," he added. Thus, he said he’d take the game’s concept and adapt it for the weaker 2600 hardware, which got the thumbs-up.

The resulting game was a weird twist on Space Invaders’ style of shooting from behind a protective barrier, and it hinged on something Warshaw desperately wanted the game to have a full-screen explosion, triggered whenever players killed the game’s major villains with a super missile. Trouble was, controlling the ship’s movement, direction, and both basic and super attacks was too much to fit onto the 2600’s limited controller. Eventually, Warshaw figured it out: "I switched from a controller button to a gameplay mechanic" to trigger the super missile. "You give the player more to do and increase the drama and complexity of the game that way."

Warshaw also talked about making an entire game fit into 4 kilobytes, and he credited his educational upbringing as an economist for that. "It taught me how to find bold-faced, cheaper ways of doing things," Warshaw said. "I threw graphics into sound and color registers. I stole stack registers to save cycles. And scores? We don’t need a score... display. Who cares what your score is? If your play is immersive, you’re paying attention to what you do in the game."

As far as interacting with Atari’s sales and marketing teams, Warshaw didn’t experience much friction. He even told a story of how he convinced Atari to go with his dream game name, by telling one marketing employee that it was named after Atari’s founder, Ray Kassar ("Yar" being Ray backwards), then swearing that employee to secrecy about the fact that Kassar was in on the name a flat-out lie. "This guy is going to run back and tell everyone," Warshaw said, and indeed, the forbidden fib swayed the entire department.

After Yars’ success, Warshaw went on to make two Steven Spielberg-related games for Atari, one of which didn’t do all that well. After that, the programmer trained to become a therapist, and he said it made perfect sense to take that route. "Being a therapist, or a game programmer, is all systems engineering," he said. "I’ve moved on to a more complex machine, is the way I look at it."

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FCC Confirms New Net Neutrality Rules Give Government Control Over Internet Rates

Federal Communications Commissioners testifying before Congress Wednesday admitted that the agency s new net neutrality rules give the FCC the authority to influence rates charged by Internet service providers.

All five commissioners appeared before a Senate panel Wednesday afternoon to testify on a number of issues currently before the FCC, including its newly adopted Internet authority. It was FCC Chairman Tom Wheeler s second appearance before Congress this week over the agency s new authority.

That authority, included in the strongest rules ever placed over ISPs in a partisan FCC vote last month, includes a provision downplayed by the agency s three Democratic commissioners, all of whom continue to combat criticism from the right that the rules give the government a regulatory heavy hand over the Internet industry.As Republican Commissioners Ajit Pai and Michael O Rielly have pointed out since Wheeler distributed his plan internally in February, the plan and provision in question doesn t explicitly set rates, but instead gives the FCC the authority to act in any way the agency deems   just and reasonable to resolve charge disputes raised by consumers.

The commissioners and Republicans in Congress argue that and other provisions included in the rules threaten to stifle industry growth and innovation, as well as implement new taxes on ISPs and Internet content creators, which will be reflected back on consumers.

 We have an obligation, I believe, to look at any complaint, anything filed before us, and make that decision accordingly, Democratic Commissioner Mignon Clyburn said in response to a question from Senate Commerce, Science, and Transportation Committee Chairman John Thune. Thune s committee oversees the FCC in the upper chamber.

Clyburn added that any complaint would have to meet an extremely high bar for the FCC to take action in the form of regulating a company s rates.

 We don t have such a case before us right now, fellow Democratic Commissioner Jessica Rosenworcel said. But I think it s a matter of due process that any provider has the opportunity to come to the commission and seek resolution.

 If a case is brought forward, it strikes me at least that the FCC has an obligation to respond, Thune said. I d have a hard time explaining how that adjudicatory process would not be rate regulation.

Thune added he thought the FCC was acted as a potentially threatening and unpredictable agency when it passed what Wheeler himself called the strongest open internet protections ever proposed last month without releasing them to the public first, as is standard FCC practice.

 Rather than exercising regulatory humility, the three majority commissioners chose to take the most radical, polarizing and partisan path possible, Thune said. Simply put, your actions jeopardize the open Internet that we are all seeking to protect.

Under the plan, the FCC will regulate ISPs under a modernized interpretation of Title II of the 1996 Telecommunications Act   a regulatory proposal inspired by those used to break up telephone monopolies in the 1930s.

Under Wheeler s 21st century Title II, the FCC will bar companies from segregating or blocking Internet content, establishing fast and slow lanes for web traffic or requiring Internet content creators to set up special deals and pay higher prices for acceptable transmission speeds.

Thune is currently working on a bill that would grant many of the protections called for by net neutrality activists, while abstaining from the public utility-style regulation adopted by the FCC last month.

China Finally Admits It Has Army of Hackers

China finally admits it has special cyber warfare units   and a lot of them.

>From years China has been suspected by U.S. and many other countries for carrying out several high-profile cyber attacks, but every time the country strongly denied the claims. However, for the first time the country has admitted that it does have cyber warfare divisions   several of them, in fact.

In the latest updated edition of a PLA publication called The Science of Military Strategy, China finally broke its silence and openly talked about its digital spying and network attack capabilities and clearly stated that it has specialized units devoted to wage war on computer networks.

An expert on Chinese military strategy at the Center for Intelligence Research and Analysis, Joe McReynolds told TDB that this is the first time when China has explicit acknowledged that it has secretive cyber-warfare units, on both the military as well as civilian-government sides.

According to McReynolds, China has three types of operational military units:

Specialized military forces to fight the network - The unit designed to carry out defensive and offensive network attacks.

Groups of experts from civil society organizations - The unit has number of specialists from civilian organizations   including the Ministry of State Security (its like China s CIA), and the Ministry of Public Security (its like FBI)   who are authorized to conduct military leadership network operations.

External entities - The unit sounds a lot like hacking-for-hire mercenaries and contains non-government entities (state-sponsored hackers) that can be organized and mobilized for network warfare operations.

According to experts, all the above units are utilized in civil cyber operations, including industrial espionage against US private companies to steal their secrets.

"It means that the Chinese have discarded their fig leaf of quasi-plausible deniability," McReynolds said. "As recently as 2013, official PLA [People’s Liberation Army] publications have issued blanket denials such as, ’The Chinese military has never supported any hacker attack or hacking activities.’ They can’t make that claim anymore."

In 2013, American private security firm Mandiant published a 60-page report that detailed about the notorious Chinese hacking group ’Unit

61398’, suspected of waging cyber warfare against American companies, organizations and government agencies from or near a 12-story building on the outskirts of Shanghai.

The UNIT 61398 also targeted a number of government agencies and companies whose databases contain vast and detailed information about critical United States infrastructure, including pipelines, transmission lines and power generation facilities.

Last year, the United States filed criminal charges against five Chinese military officials, named Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, for hacking and conducting cyber espionage against several American companies.

The alleged hackers were said to have worked with the PLA s Unit 61398 in Shanghai. Among spying on U.S companies and stealing trade secrets, they had also accused for stealing information about a nuclear power plant design and a solar panel company s cost and pricing data.

Proofpoint Uncovers Internet of Things (IoT) Cyberattack

Proofpoint, Inc., a leading security-as-a-service provider, has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks. As the number of such connected devices is expected to grow to more than four times the number of connected computers in the next few years according to media reports, proof of an IoT-based attack has significant security implications for device owners and Enterprise targets.

Just as personal computers can be unknowingly compromised to form robot-like "botnets" that can be used to launch large-scale cyberattacks, Proofpoint’s findings reveal that cyber criminals have begun to commandeer home routers, smart appliances and other components of the Internet of Things and transform them into "thingbots" to carry out the same type of malicious activity. Cyber criminals intent on stealing individual identities and infiltrating enterprise IT systems have found a target-rich environment in these poorly protected internet connected devices that may be more attractive and easier to infect and control than PC, laptops, or tablets.

The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide. More than 25 percent of the volume was sent by things that were not conventional laptops, desktop computers or mobile devices; instead, the emails were sent by everyday consumer gadgets such as compromised home-networking routers, connected multi-media centers, televisions and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location   and in many cases, the devices had not been subject to a sophisticated compromise; instead, misconfiguration and the use of default passwords left the devices completely exposed on public networks, available for takeover and use.

"Bot-nets are already a major security concern and the emergence of thingbots may make the situation much worse" said David Knight, General Manager of Proofpoint’s Information Security division. "Many of these devices are poorly protected at best and consumers have virtually no way to detect or fix infections when they do occur. Enterprises may find distributed attacks increasing as more and more of these devices come on-line and attackers find additional ways to exploit them."

While IT experts have long predicted security risks associated with the rapidly proliferating Internet of Things (IoT), this is the first time the industry has reported actual proof of such a cyber attack involving common appliances   but it likely will not be the last example of an IoT attack. IoT includes every device that is connected to the internet - from home automation products including smart thermostats, security cameras, refrigerators, microwaves, home entertainment devices like TVs, gaming consoles to smart retail shelves that know when they need replenishing and industrial machinery   and the number of IoT devices is growing enormously. IDC predicts that more than 200 billion things will be connected via the Internet by 2020 . But IoT devices are typically not protected by the anti-spam and anti-virus infrastructures available to organizations and individual consumers, nor are they routinely monitored by dedicated IT teams or alerting software to receive patches to address new security issues as they arise. The result is that Enterprises can’t expect IoT-based attacks to be resolved at the source; instead, preparations must be made for the inevitable increase in highly distributed attacks, phish in employee inboxes, and clicks on malicious links.

"The ’Internet of Things’ holds great promise for enabling control of all of the gadgets that we use on a daily basis. It also holds great promise for cybercriminals who can use our homes’ routers, televisions, refrigerators and other Internet-connected devices to launch large and distributed attacks", said Michael Osterman, principal analyst at Osterman Research. "Internet-enabled devices represent an enormous threat because they are easy to penetrate, consumers have little incentive to make them more secure, the rapidly growing number of devices can send malicious content almost undetected, few vendors are taking steps to protect against this threat, and the existing security model simply won’t work to solve the problem."

Double FREAK! A Cryptographic Bug That Was Found Because of The FREAK Bug

Imagine that you just checked into a hotel.

You’re in the lift on the way to your room, holding a key.

You get to your room; you wave, swipe or turn the key; and the door opens.

Assuming the door wouldn’t open until you presented the key, it certainly feels like security of a sort, doesn’t it?

But what if your key isn’t unique?

What if your key opens every other door in the hotel (or, for that matter, if every other key opens your door)?

How would you ever know, just for starters?

You could make a habit of trying your key on a random selection of doors every time you use a hotel, but even that might not help, because:

You’ll probably get into trouble, especially if you do manage to open someone else’s door unexpectedly.

Some hotels only let you access your own floor, so you’ll never know if your key might open doors on other floors.

Your key might be fine until the hotel next reboots its lock control server.

Other keys might open your door, even if your key doesn’t open other people’s.

In short, you have to assume that the hotel’s key management software (or its locksmith service) knows what it’s doing.

Now imagine you just finished setting up a secure router at home or at work, taking it out of its box, putting it through its first-time setup, and connecting it to the network.

You might similarly assume that tasks related to key setup, such as generating public-private keypairs, were done correctly.

In fact, history suggests that key creation tasks sometimes aren’t done well at all, especially on small, cheap routers where generating pseudorandom numbers is hard to do well because there just aren’t many sources of unpredictable data inside the router’s limited hardware.

If the clock always sets itself, say, to 01:00 on 01 January 1991, every time you power up, then randomisation routines that rely on the time of day to mix things up at the outset are not going to get very mixed up at all.

But what if conventional checks showed you that your router’s cryptographic keys looked OK, or at least that on the 10 routers you just deployed, all the keys were dfferent?

You’d probably be reasonably happy that their "room keys" wouldn’t open each other’s doors.

Researchers at Royal Holloway, a UK institution already well-known for its cryptographic work, found that your happiness might be misplaced.

What’s more, they found out sort-of by mistake, though we don’t mean to denigrate their work by putting it that way.

They decided to use a fast network scanner called Zmap to check up on the FREAK vulnerability, and measure how many servers still needed patching.

FREAK, of course, is a recently-reported security bug that allows an attacker to trick each end of a TLS (secure) internet connection into dropping back to a level of encryption that is rather easy to break these days.

FREAK involves going back to 512-bit RSA keys, a size that was already successfully cracked by civilian researchers with unexceptional equipment back in 1999.

And Zmap is a special type of internet scanning tool that can, in theory, make a probe to almost every active computer on the internet within one hour.

Just the combination for a Friday afternoon experiment in a cryptography lab!

The team quickly measured that just under 10% of servers on the internet were still vulnerable to FREAK.

Useful information.

A little disappointing, perhaps, because by now you might expect the proportion to be much lower; but also somewhat encouraging, because the original FREAK report, released two weeks ago, put the figure at 26%.

If that was all the researchers had found, you might already consider this objective measurement to be "a good return on investment for a Friday afternoon’s work," to borrow the authors’ own words.

But there’s more.

While they were about it, the researchers noticed that a surprising number of servers that were FREAKable presented exactly the same 512-bit RSA key when they were tricked into falling back to old-style encryption.

As it happens, many servers cheat a little bit with RSA keys, because generating a public-private keypair is a lot slower than merely using that keypair for encryption and decryption.

So, instead of generating a unique keypair for every connection, they only generate a keypair when the server starts up, and keep on using it until the server is restarted.

In theory, someone who grabs your private key could then decrypt every connection that was protected with it, which increases the risk compared to creating a new keypair every time.

But the idea is that if a crook gets into your server and acquires your temporary private key, then all security bets are off anyway, so this can be considered an acceptable risk.

What is definitely not an acceptable risk is sharing keypairs with other servers in other locations belonging to other organisations.

Otherwise, if any one of the others were hacked (or maliciously revealed the private key to cybercrooks), then you’d fall along with them.

In the Royal Holloway paper, the authors found that one particular 512-bit RSA key, exposed during FREAK testing, was repeated a whopping 28,394 times.

That’s an awfully big hotel to have the same key for every door!

Worse still, that repeated key seemed to belong to a VPN router product.

Ironically, a VPN is a Virtual Private Network   a secure, encrypted network "tunnel" that is supposed to let your remote workers connect back to head office in much greater safety than if they were to use the open internet.

Does it matter?

You’re probably thinking, "Why fuss about repeated RSA keys if those keys only show up during a FREAK attack, which is a bug in its own right anyway?"

The point is that the repeated-key bug reveals that, somewhere in those affected VPN routers, there exists an egregious programming mistake to do with cryptographic randomness.

That bug could affect other aspects of the router’s encryption setup code. Yet the researchers only spotted that bug because they happened to be looking for a completely different one.

There are two important take-aways here:

Finding programming mistakes is hard; sometimes it requires serendipitous coincidences.

If you are the vendor of the affected router (check yours: you’ll soon see if it’s you), you have a code review to do.

Silk Road Lieutenant Peter Nash Pleads Guilty

An Australian man who worked as the main moderator of the underground Silk Road online drugs, guns and dirty deeds bazaar has pleaded guilty to money laundering and drug trafficking charges in the US.

Peter Phillip Nash, 42, who went by the tag "Samesame butdifferent" and whose other aliases included Batman73, Symmetry and Anonymousasshit, was arrested in Brisbane in December 2013 and extradited to the US in November 2014.

Nash filed his guilty plea on Friday in Manhattan federal court.

According to the indictment, Nash worked as Silk Road’s primary moderator for 10 months, from January until October 2013.

US authorities allege that Nash was paid between $50,000 and $75,000 a year (approximately £35,000 to £50,000) to act as the marketplace’s primary moderator, although, as Reuters reports, Nash told the court he only pocketed about $30,000 (about £20,000).

He used that to buy drugs, he said - just part of what he told the court he now regrets:

I deeply regret my conduct and any consequent harm I caused.

Nash said he first became involved with Silk Road when buying drugs for friends

He told the court that he had never found out the real identity of Ross

Ulbricht, the site’s founder.

The 30-year-old Ulbricht, who went by the tag "Dread Pirate Roberts", launched the site, which was hidden on the Tor network, in early 2011.

In February, Ulbricht was convicted on seven criminal counts by a Manhattan federal jury and could face life in jail.

The US Department of Justice (DOJ) has said that over the two-and-a-half years that Silk Road was running, it facilitated transactions of hundreds of kilograms between drug dealers and more than 100,000 buyers - transactions valued at over $200 million, all paid in Bitcoin.

Silk Road was taken down in October 2013.

The site didn’t only deal in drugs.

At the time of Ulbricht’s original indictment in early 2014, the Manhattan US attorney claimed that alongside 13,000 posts selling "controlled substances", the site also carried over 800 adverts for "Digital Goods" including malware and pirated software, 169 for forged documents including passports and driver’s licenses, and 159 "Service" listings.

The services included malware, hacking-for-hire and murders-for-hire. Ulbricht is alleged to have made six attempts to arrange murders in order to protect the site, although no evidence has pointed to the murders having been carried out.

In fact, Ulbricht hired one hitman who turned out to be an undercover agent.

Ulbricht plans to appeal his verdict.

Two other alleged former Silk Road staff members are also facing trial: Andrew Jones, who pleaded guilty on 2 October 2014 and is due to be sentenced later this year, and Gary Davis, who’s now out on bail in Ireland and is awaiting the conclusion of extradition proceedings.

Nash will face sentencing on 26 May 2015. The maximum penalty under US federal sentences for drug trafficking is life in prison, with a minimum of 10 years when more than 5kg of cocaine or 1kg of heroin is involved.

Google Forgets One Little "Yes/No" Setting, Leaks Private WHOIS Data

Google is quite the collector when it comes to data.

As we well know, sometimes the Mountain View juggernaut sometimes drives right to the brink of controversy, and occasionally right over it.

Nevertheless, for all the dodgy Wi-Fi sniffing and sneaky pharmaceutical promotion, the ad giant has typically been considered a safe pair of hands when it comes to data leakage.

Google may hoover up more about you than you know about yourself, but it hasn’t had any major breach or data spillage moments like Target, Adobe or Sony.

There were some admittedly amateur-time coding flaws revealed in Android in 2014, but as far as network security goes, Google has set itself up as a bit of a leader.

For example, there was the switch to HTTPS and nothing but for Gmail, and the company’s timely blanket shift to 2048-bit RSA keys.

And during a fierce internet freedom dispute in Turkey in 2014, Google’s free, unregulated, public DNS servers (at 8.8.8.8 and 8.8.4.4) became the special favourites of Turkish activists.

But even Google can make mistakes, as network security expert group Talos recently noticed.

In this case, the result was apparently a large-scale leak of data that Google had promised to keep to itself.

The leakage had to do with what’s known as WHOIS data, the information about who’s who on the internet.

When you register a domain name to give yourself a human-friendly location in the internet universe, most countries require you to say who you are.

Legitimate companies and honest individuals often make that information public:

But many domain name service (DNS) registrars offer privacy protection.

Even though the registrar knows who you are, and where you live, for accountability reasons, it shields that information from the rest of the world, for privacy reasons:

The comparative ease with which crooks can harvest WHOIS data, which includes names, physical addresses and phone numbers, makes DNS privacy protection well worth considering, especially for small businesses and individuals.

What Talos spotted is that domains registered for Google Apps through a registrar called eNom underwent a strange, and at first unexplained, change near the beginning of 2013.

For years, the proportion of customers requesting privacy protection remained fairly constant, at about 90%.

That started to change rapidly in 2013, until by the start of 2015, about 99% of customers were *not* using privacy protection.

The explanation turned out to be very simple.

When eNom customers renewed a protected Google Apps domain, the protection was lost, apparently due to Google sending incorrect data back at the end of the renewal process.

In other words, what amounted to a single-bit error   Protected? (Y/N) blew the cover of customers who had requested privacy for their registration data.

What to do?

If you were one of the affected customers, there isn’t a lot you can do now to "unreveal" your data.

That’s the thorny problem of data breaches: how to re-hide data that can’t be changed easily, or even at all, like your physical address or your birthday.

Anyone who did a WHOIS query against your domain name while it was non-private now has your data, and may end up keeping it as part of the internet’s historical record.

Nevertheless, this incident does remind us of one thing: if you have data that you have deliberately opted out of making public, it’s worth checking, as regularly as you can, to make sure that you remain opted out.

The earlier you spot any mistakes   much like realising you are listed in the phonebook when you weren’t supposed to be   the earlier you can try to get the mistake reversed.

Also, if your data was revealed as part of a more general operational error (which seem to be what happened here), the sooner someone says something, the better for everyone else, especially those who haven’t been affected yet.

Think of checking for and reporting privacy glitches partly as a protective move for yourself, and partly as an altruistic move for the rest of us!

OpenSSL To Patch High Severity Vulnerability This Week

The OpenSSL Foundation is set to release a handful of patches for undisclosed security vulnerabilities in its widely used open source software later this week, including one that has been rated "high" severity.

In a mailing list note published last night, Matt Caswell of the OpenSSL Project Team announced that OpenSSL versions 1.0.2a, 1.0.1m, 1.0.0r, and 0.9.8zf will be released Thursday.

"These releases will be made available on 19th March," Caswell wrote. "They will fix a number of security defects. The highest severity defect fixed by these releases is classified as "high" severity."

OpenSSL is an open-source implementation of the SSL and TLS protocols. It’s a technology that’s widely used by almost every websites to encrypt web sessions, even the Apache web server that powers almost half of the websites over the Internet utilizes OpenSSL.

Further details on the mystery security vulnerabilities (CVE-2015-0209, CVE-2015-0285, CVE-2015-0288) are unavailable at this time, although some industry experts have speculated that this high severity flaw could be another POODLE or Heartbleed bug, worst TLS/SSL flaws that are still believed to be affecting websites on Internet today.

Heartbleed was discovered in April last year in an earlier version of OpenSSL, which allowed hackers to read the sensitive contents of users’ encrypted data, such as credit card transactions and even steal SSL keys from Internet servers or client software.

Also, in June the same year a serious Man-in-the-Middle (MITM) vulnerability was discovered and fixed by the OpenSSL Project Team. However, the vulnerability wasn’t quite as severe as the Heartbleed flaw, but it’s serious enough to decrypt, read or manipulate the encrypted data, particularly affecting Android users.

Months later, another critical flaw, POODLE - Padding Oracle On Downgraded Legacy Encryption - was discovered in the decade old but widely used Secure Sockets Layer (SSL) 3.0 cryptographic protocol that could allowed hackers to decrypt the contents of encrypted connections to websites.

More recently, a new flaw, dubbed FREAK - Factoring Attack on RSA-EXPORT Keys - discovered that allowed an attacker to force SSL clients including OpenSSL, to downgrade to weaken ciphers that can be easily broken, potentially allowing them to eavesdrop on encrypted networks by conducting Man-in-the-Middle attacks.

Almost every big brand was affected by the dangerous FREAK flaw, including Apple and Android smartphone devices, BlackBerry devices and cloud services, as well as every version of Windows operating system.

So, OpenSSL is an important software project and is ranked first under the Linux Foundation s Core Infrastructure Initiative given its widespread use and lack of in-depth security review.

Major companies, including Google, Facebook, and Cisco, are funding the Internet’s "Core Infrastructure Initiative," a US$2 Million-a-year project dedicated to supporting and auditing open-source projects.

Facebook Clarifies Guidelines on Acceptable Posts

Facebook on Monday updated its "community standards" guidelines, giving users more clarity on acceptable posts relating to nudity, violence, hate speech and other contentious topics.

The world’s biggest social network said it does not allow a presence from groups advocating "terrorist activity, organized criminal activity or promoting hate."

The new guidelines say Facebook will take down "graphic images when they are shared for sadistic pleasure or to celebrate or glorify violence."

Nudity is also removed in many cases but allowed for images of breastfeeding, art or medical conditions.

"These standards are designed to create an environment where people feel motivated and empowered to treat each other with empathy and respect," said a blog post from Facebook global policy chief Monika Bickert and deputy general counsel Chris Sonderby.

"While our policies and standards themselves are not changing, we have heard from people that it would be helpful to provide more clarity and examples, so we are doing so with today’s update."

The new guidelines say Facebook members should use their "authentic name," a move that appears to head off criticism from people who used stage or performance names instead of their legal name.

In October Facebook said it would ease its "real names" policy that prompted drag queen performers to quit the social network and sparked wider protests in the gay community and beyond.

Facebook’s new guidelines said it would remove content, disable accounts and work with law enforcement "when we believe that there is a genuine risk of physical harm or direct threats to public safety."

But it also pointed out "that something that may be disagreeable or disturbing to you may not violate our community standards."

The move comes with Facebook and other social media struggling with defining acceptable content and freedom of expression.

"It’s a challenge to maintain one set of standards that meets the needs of a diverse global community," the blog post said.

"This is particularly challenging for issues such as hate speech. Hate speech has always been banned on Facebook, and in our new community standards, we explain our efforts to keep our community free from this kind of abusive language."

Facebook said earlier this year it was putting warnings on "graphic content," which would also be banned for users under 18. In 2013, Facebook ended up banning a beheading video after outrage followed a lifting of the ban.

Twitter meanwhile has become the latest online platform to ban "revenge porn," or the posting of sexually explicit images of a person without consent.

Twitter faced threats after blocking accounts linked to supporters of the Islamic State, but one study showed at least 46,000 Twitter accounts have been linked to the group.

Facebook at the same time released its report on government requests for user data in the second half of 2014, showing a modest uptick to 35,051 from 34,946 in the prior period.

"There was an increase in data requests from certain governments such as India, and decline in requests from countries such as the United States and Germany," the blog post said.

The amount of content restricted for violating local law increased by 11 percent 9,707 cases from 8,774.

"We saw a rise in content restriction requests from countries like Turkey and Russia, and declines in places like Pakistan," Facebook said.

Facebook Revamps Community Guidelines,
Shows What The Social Network Will Take Down

Facebook has revamped the social network’s community standards and guidelines to show what registered accounts can (and more importantly, cannot) share on the service.

Changes made to the guidelines also clarify the company’s position on bullying, threats of violence and even hate speech. In a new blog post, Facebook’s Monika Bickert, Head of Global Policy Management, and Chris Sonderby, Deputy General Counsel, go into some detail about prohibiting harassment, threatening violence, and any hate speech against someone because of their race or religious beliefs.

The new standards are fairly light to read through too. For example, according to the new guidelines provided, Facebook will allow some degree of nudity.

"We remove photographs of people displaying genitals or focusing in on fully exposed buttocks. We also restrict some images of female breasts if they include the nipple, but we always allow photos of women actively engaged in breastfeeding or showing breasts with post-mastectomy scarring. We also allow photographs of paintings, sculptures and other art that depicts nude figures."

As always, Facebook will continue reviewing reported content to maintain freedom to share ideas, and to prevent content from being pulled due to incorrect reporting or a specific country requesting said content to be removed. If a piece of content has been reported as illegal in a region, Facebook would look to prevent people in the affected area from accessing the media in favour of flat out removal.

Facebook also touched on data requests from governments and how the company has actually witnessed a decline in submissions from the US.

"The number of government requests for account data remained relatively flat, with a slight increase to 35,051 from 34,946. There was an increase in data requests from certain governments such as India, and decline in requests from countries such as the United States and Germany."

They close by stating they will continue pushing governments to reform surveillance practices. It’s a delicate balance between freedom of speech and keeping those who use Facebook safe online. You can check out the new community standards section of the Facebook website for more details.

Fully Patched Versions of Firefox, Chrome, IE 11 and Safari Exploited at Pwn2Own Hacking Competition

As in years past, the latest patched versions of the most popular web browsers around stood little chance against those competing in the annual Pwn2Own hacking competition. The usual suspects   Apple Safari, Google Chrome, Mozilla Firefox and Microsoft Internet Explorer   all went down during the two-day competition, earning researchers a collective total of $557,500 in prize money.

The event, which took place at the CanSecWest conference in Vancouver, was sponsored by the Hewlett-Packard Zero Day Initiative. During the first day, HP awarded $317,500 to researchers that exploited flaws in Adobe Flash, Adobe Reader, Internet Explorer and Firefox.

eWeek notes that the first reward, paid to a hacker by the name of ilxu1a, was for an out-of-bounds memory vulnerability in Firefox. It took less than a second to execute which earned him a cool $15,000.

Firefox was exploited twice during the event. Daniel Veditz, principal security engineer at Mozilla, said the foundation was on hand during the event to get the bug details from HP. Engineers are already working on a fix back at home, he added, that could be ready as early as today.

Another security researcher, JungHoon Lee, managed to demonstrate exploits against Chrome, IE 11 and Safari. As you can imagine, he walked away with quite a bit of money: $75,000 for the Chrome bug, $65,000 for IE and $50,000 for the Safari vulnerability. He also received two bonuses totaling $35,000.

Spartan, Microsoft’s Internet Explorer "Alternative"

Look out, Internet Explorer. After 20 years of competing against rival web browsers, Microsoft is gearing up to launch its own alternative to its once-dominant Internet surfing program.

Microsoft has built a new web browser designed for the modern web and mobile devices to go with its new Windows 10 operating system that’s coming later this year. Explorer will still be available, but Microsoft hinted this week that its new   and as-yet unnamed   browser will get top billing in the future.

"They want to be associated with something sexy and new," said tech analyst Al Hilwa, who follows Microsoft and other software companies for International Data Corp. "Explorer has gotten kind of a bad reputation for not being as fast as the Chromes and Firefoxes of this world," he said, referring to rival browsers from Google and Mozilla.

Though exact estimates vary, market researchers say Explorer has been outpaced by Chrome in recent years as the world’s most widely used web browser. While some analysts say Explorer is still the leader on desktop PCs, it lags far behind browsers made by Google, Mozilla and Apple for smartphones and tablets.

Explorer isn’t going away completely, however. Many businesses use web-based software that relies on Explorer. Microsoft will likely support both Explorer and the new browser for several more years, so it doesn’t alienate business customers by forcing them to rebuild their systems from scratch, Hilwa said.

Microsoft unveiled the new browser, known inside the company as "Project Spartan," at a January press event. Corporate Vice President Joe Belfiore touted features designed to make it easier for users to view web pages, save them or share comments about them with friends. Even then, the company said it would continue offering Explorer with the new version of Windows.

But the tech world took note this week when Microsoft marketing chief Chris Capossela told a tech conference in Atlanta that the company is in the process of choosing a new name that won’t include the word "Explorer"   underscoring the difference from previous browser updates that were simply assigned numbers, such as Internet Explorer 11.

Microsoft didn’t invent the web browser, but it has invested heavily to promote Explorer since it was first launched in 1995. The company even had to answer government charges in the 1990s that it competed unfairly against the once-popular Netscape browser by combining Explorer with earlier versions of Windows.

In an industry that values the new and looks down on the old, Microsoft appears to be signaling Explorer’s diminished status as a "legacy" product. Microsoft is betting heavily that its new Windows 10 software will appeal to computer users who are increasingly using mobile devices.

And in a terse statement, the company said Wednesday: "Project Spartan is Microsoft’s next generation browser, built just for Windows 10. We will continue to make Internet Explorer available with Windows 10 for enterprises and other customers who require legacy browser support."

Say Hello to Windows 10 This Summer and Goodbye to Passwords

Microsoft has put Windows 10 on the fast track saying in an unexpected announcement the new OS will arrive this summer. That’s a surprise escalation in expectations from the fall timeline targeted by Microsoft Chief Operating Officer Kevin Turner back in December.

The company announced the unexpected earlier delivery date at the Windows Hardware Engineering Conference (WinHEC), taking place in Shenzhen, China this week. Also at WinHEC, as reported yesterday, Microsoft revealed that the release of Windows 10 will aim at transitioning users away from passwords to login to their systems and instead will offer Microsoft’s new biometric authentication tool called Windows Hello.

While it wasn’t initially clear to what extent the Windows Hello technology would be supported in Windows 10, Terry Myerson, executive vice president for the Windows platform group at Microsoft said at WinHEC and in a blog post that all OEMs have agreed to support it.

Windows 10 will be available in 190 countries and 111 languages when it launches, according to Myerson. Obviously that’s a wide window given it can arrive anytime between June 21 and Sept. 20. But the expedited release may suggest that Microsoft doesn’t want to miss this year’s back-to-school season, a time many students buy new systems. If that’s the case, it will need to come in June or July, rather than late September.

The big question an earlier-than-expected release raises: is Microsoft looking to rush Windows 10 out the door too soon and will it come out feature-complete? Meanwhile, there are many new features testers have yet to see, such as the new browser component called Spartan and yesterday’s reveal: Windows Hello. Joe Belfiore, corporate vice president for Microsoft’s operating systems group unveiled Windows Hello at WinHEC, which he said provides system-level support for biometric authentication, including fingerprint and facial recognition as a replacement for passwords.

Hello isn’t the first effort to bring biometrics to Windows PCs. Makers of PCs have offered fingerprint scanners on a small selection of their PCs for years now. But few used them and most devices today have done away with them. This time, it looks like Microsoft is aiming for biometrics that will be pervasive in Windows 10 devices. "We’re working closely with our hardware partners to deliver Windows Hello-capable devices that will ship with Windows 10," Myerson said. "We are thrilled that all OEM systems incorporating the Intel RealSense F200 sensor will fully support Windows Hello, including automatic sign-in to Windows."

Myerson said Microsoft is also offering a new version of Windows for smaller Internet of Things devices ranging from ATM machines to medical equipment thanks to partnerships with the Raspberry Pi Foundation, Intel, Qualcomm and others. Microsoft also unveiled Qualcomm’s DragonBoard 410C for Windows 10 devices. It includes the first Windows 10 developer board that’s integrated with Wi-Fi, Bluetooth and GPS, along with the Qualcomm Snapdragon 410 chipset.

Pirates, Beware of That Free Windows 10 Upgrade!

Microsoft earlier this week revealed that it plans to offer Windows pirates a free upgrade to Windows 10, even if they do not own a genuine copy of a Windows version eligible to receive the update free of charge. Initially, it wasn t clear whether the policy applies to anyone currently stealing Windows, or only to Chinese pirates. Ars Technica has learned more details on the matter, revealing that the free update isn t necessarily the good news pirates may have been expecting.

The publication says that ZDNet has confirmed the update path for illegal Windows copies applies to pirates everywhere, not just in China. This rather lax policy towards piracy might also encourage certain users to already take advantage of Microsoft s intentions by installing a non-genuine Windows version on their devices and just wait for the final Windows 10 build to be released.

But once the Windows 10 upgrade is installed over a non-genuine Windows 7 or Windows 8.x version, that computer will keep being considered non-genuine by Microsoft.

With Windows 10, although non-Genuine PCs may be able to upgrade to Windows 10, the upgrade will not change the genuine state of the license   the company told Ars. If a device was considered non-genuine or mislicensed prior to the upgrade, that device will continue to be considered non-genuine or mislicensed after the upgrade.

It s not clear what the repercussions might be after the Windows 10 upgrade is installed on a non-licensed device. The publication asked Microsoft for clarification on the material implications of getting a non-genuine upgrade, but the company did not elaborate on the matter.

Therefore, anyone planning to take advantage of this loophole towards obtaining a free Windows 10 copy   that s installing a pirated copy of Windows on a computer and then simply updating it to Windows 10   should think twice about what the potential implications might be.

No, Microsoft Isn’t Giving Free, Legitimate Windows 10 Upgrades to Pirates

Earlier this week, Microsoft told Reuters that it would provide free

Windows 10 upgrades to people running genuine and non-genuine versions of Windows when the new operating system comes out this summer.

Translated from geek speak, it sounded as if Microsoft would be giving everyone, even people running pirated versions of Windows, the option to upgrade to Windows 10 for free. Many publications, including Yahoo Tech, reported that pirates would be given amnesty for their stolen versions of Windows and be given, for free, a licensed version of Windows 10.

If that sounds too good to be true, it is.

When Terry Myerson, head of Microsoft s Operating Systems group, made the announcement, he left out a specific but important caveat, which is that any upgrade from a pirated version of Windows would be registered as non-genuine. In other words, the upgrades won t be legit in Microsoft s books.

If you ve ever used a non-genuine version of Windows and tried to upgrade it, you ve likely noticed that as soon as Microsoft s servers see that your copy of Windows is illegitimate, the desktop flashes black and adds bars that tell you your Windows install is non-genuine. You also get a ton of annoying notifications telling you to upgrade to genuine Windows.

Obviously, pirated versions of Windows are apt to carry malicious software, given that they usually come from unknown sources via peer-to-peer networks.

If you re running a non-genuine version of Windows 7 or 8, Microsoft still lets you download critical security updates   better to keep everyone safe   but you can t get optional updates or use Microsoft s built-in Windows Defender security software.

Microsoft hasn t said how it will handle non-genuine versions of Windows 10, which means that we don t know if those using non-genuine versions will have access to security updates.

Here s what Microsoft told us about the matter:

 We have always been committed to ensuring that customers have the best Windows experience possible. With Windows 10, although non-Genuine PCs may be able to upgrade to Windows 10, the upgrade will not change the genuine state of the license. Non-Genuine Windows is not published by Microsoft. It is not properly licensed, or supported by Microsoft or a trusted partner. If a device was considered non-genuine or mislicensed prior to the upgrade, that device will continue to be considered non-genuine or mislicensed after the upgrade. According to industry experts, use of pirated software, including Non-Genuine Windows, results in a higher risk of malware, fraud (identity theft, credit card theft, etc), public exposure of your personal information, and a higher risk for poor performance or feature malfunctions.

So, yes, you ll be able to upgrade your pirated version of Windows 7 or 8 to Windows 10, but it s not going to be a full-on legitimate upgrade, and there s no guarantee that you ll still be able to get all of the important software updates you ll need.

A Third of Americans Have Changed Online and Phone behaviors Post-Snowden

Edward Snowden has been heard, and his words are having at least some effect.

A Pew Research Center survey has found that nearly one third of American adults have taken steps to protect their information from government surveillance programs that monitor phone and digital communications.

Most - 87% - of Americans have heard about the National Security Agency’s (NSA’s) surveillance programs since Snowden began leaking documents nearly two years ago.
More than one fifth - 22% - say that they’ve since changed their use of various technology tools "a great deal" or "somewhat".

Between late November and early January, The Pew Center surveyed 475 adult members of the GfK Knowledge Panel: a consumer research company. It also surveyed 59 panelists who participated in one of six online focus groups conducted during December 2014 and January 2015.

57% reported that they consider surveillance of US citizens to be unacceptable, while 54% think it’s justifiable when those being monitored are either politicians or from other countries.

Out of those surveyed who are at least somewhat aware of the NSA’s surveillance programs (30% of adults), 34% have taken at least one step to keep their information hidden or shielded from the government.

Specifically, here’s what they’re doing:

25% are using more complex passwords
17% changed their privacy settings on social media
15% use social media less often
15% have avoided certain apps
13% have uninstalled apps
14% say they speak more in person instead of communicating online or on the phone
13% have avoided using certain terms in online communications
Another 25% of those aware of the surveillance programs (22% of surveyed adults) have changed how they interact with communication technology "a great deal" or "somewhat".

Specifically:

18% say they’ve changed the way they use email
17% have changed the way they use search engines
15% say they have changed the way they use social media sites such as Twitter and Facebook
15% have changed the way they use their cell phones
The privacy tools people are not using, and why

The Pew Center suggests that those who haven’t changed their behaviors might be intimidated by it being "somewhat" or "very" difficult to find tools and strategies that would help them be more private online and when using their mobile phones.

These are some of the commonly available tools that they reportedly aren’t using:
53% haven’t adopted or considered using a search engine that doesn t keep track of a user’s search history and another 13% don’t know about these tools.

46% haven’t adopted or considered using email encryption programs and another 31% don’t know about such programs.

43% haven’t adopted or considered adding privacy-enhancing browser plug-ins like DoNotTrackMe (now known as Blur) or Privacy Badger and another 31% don’t know about such plug-ins.

41% haven’t adopted or considered using proxy servers that can help them avoid surveillance and another 33% don’t know about them.

40% haven’t adopted or considered using anonymity software such as Tor and another 39% don’t know what it is.

Those numbers are probably on the optimistic side, the Pew Center said, given that "noteworthy" numbers of respondents answered "not applicable to me" on related questions - in spite of virtually all of them being internet and cell phone users.

The more people say they know about surveillance, the more likely that they’ve changed their behaviors: out of those who say they’ve heard a lot, 38% say they’ve changed a great deal/somewhat in at least one activity, and out of those who are at least somewhat concerned about the programs, 41% have changed at least one activity.

Specific concerns include government monitoring of social media, search engines, cell phones, apps, and email.

When it comes to the question of whether the courts are doing a good job of balancing the needs of law enforcement and intelligence agencies with citizens right to privacy, there’s a pretty even divide: 48% say courts and judges are balancing those interests, while 49% say they aren’t.

Not that Americans are adverse to all surveillance, mind you. Generally, the public approves of monitoring plenty of people, including foreign citizens, foreign leaders, and American leaders:

82% say it’s acceptable to monitor communications of suspected terrorists
60% believe it’s acceptable to monitor the communications of American leaders.
60% think it’s OK to monitor the communications of foreign leaders
54% say it’s acceptable to monitor communications from foreign citizens

So, monitoring foreigners and politicians is OK, but not US citizens: 57% say that the monitoring of citizens’ communications is unacceptable.

But then again, lots of people - 65% - think it’s OK to monitor people who pepper their communications with words such as "explosives" and "automatic weapons" in search engine queries, and 67% think it’s OK to monitor people who visit anti-American websites.

Americans are split about just how much we should worry about surveillance - particularly when it comes to their own digital behavior.

Overall, 52% say they’re "very concerned" or "somewhat concerned" about government surveillance of Americans’ data and electronic communications, compared with 46% who say they’re "not very concerned" or "not at all concerned" about surveillance.

When asked about monitoring of their own communications and online activities, the concern levels slipped:

39% describe themselves as "very concerned" or "somewhat concerned" about government monitoring of their activity on search engines.
38% say they’re "very concerned" or "somewhat concerned" about government monitoring of their activity on their email messages.
37% express concern about government monitoring of their activity on their cell phone.
31% are concerned about government monitoring of their activity on social media sites, such as Facebook or Twitter.
29% say they’re concerned about government monitoring of their activity on their mobile apps.

Can’t Remember Your Password? Here Are Two New Ways To Log In

Tired of trying to remember a different password for each of your online accounts? Or worried about re-using the same password too many times? You’re not alone. Tech experts agree that traditional passwords are annoying, outmoded and too easily hacked.

This week, Yahoo and Microsoft offered up some alternatives: Yahoo says it can text temporary passwords to users’ phones each time they want to sign into their Yahoo accounts. Microsoft says it is building facial-recognition and fingerprint-identification technology into Windows 10, the new computer operating system coming this summer, so users can log on with their fingertip or face. The two approaches drew different reviews.

Here’s what you should know:

Convenience and security. That’s what Yahoo is promising users who choose to receive a single-use password "on demand"   sent by text message to their mobile phone each time they want to sign into their Yahoo account. Once you opt into the program, there’s no more need to create or memorize a password for Yahoo’s email or other services.

Not a good move, experts say.

"Yahoo just made it easier for attackers to compromise an account," said Tim Erlin, risk strategist for the cybersecurity firm Tripwire. Temporary passwords can fall into the hands of anyone who steals your phone. While most phones can be set to require a separate password to unlock the home screen, many people don’t bother to do so. Phones can also be infected with malware that intercepts or copies text messages, he said.

Though it may be convenient, Erlin said, Yahoo’s on-demand option is a step backward from another alternative the company offers, known as two-factor authentication. With that option, users must provide both a traditional password and a one-time code that is texted to their phones. That’s considered stronger because a hacker would need both to get into a user’s account.

Yahoo security chief Alex Stamos agrees that two-factor authentication is stronger. But many people don’t use it, he said in an online post defending against critics. Instead, people too often recycle short passwords that are easier to type, especially on small phone screens, but also easy for hackers to guess, he said.

Since most online services let users reset passwords by sending a text or email to their phones, users are already vulnerable if they lose their device, Stamos argued.

"The truth is that passwords are so incredibly, ridiculously broken that it is almost impossible to keep users safe as long as we have any," Stamos wrote on his Twitter account. He said Yahoo is working on other solutions.

The concept of logging in by scanning your fingerprint or face used to seem like sci-fi. But the future is here.

Microsoft said this week that it is building "biometric authentication" technology into the next version of its Windows software, so that users can unlock computers or phones with their face, iris or fingerprint. The devices must have a fingerprint reader or a high-end camera with infrared sensors, which are becoming more common.

Windows 10 users may also be able to use their face or fingerprint to sign into other online accounts. Microsoft is providing related software to builders of independent apps and websites so they too can verify a user’s identity through a combination of biometrics and an encrypted code automatically generated by the user’s computer or phone, Microsoft Vice President Joe Belfiore wrote in a blog post.

Google already offers facial recognition as an option for unlocking Android phones, although it’s not widely used. Early versions were criticized as unreliable, but the technology has improved, said Anil Jain, a biometrics expert at Michigan State University. Apple and Samsung offer fingerprint identification to unlock some phones; Apple also uses it to authorize purchases through Apple Pay.

It’s too early to know if Microsoft’s system will be effective or gain wide acceptance, Jain cautioned. But alternatives to passwords are definitely needed, said fraud expert Al Pascual, who studies the banking and payments industry at Javelin Strategy & Research.

Too many people use the same password for multiple accounts, and they are routinely stolen by hackers.

"The password today," he said, "is more of a liability than any kind of security measure."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.